INTERNET CRIME

R L Dunne, H M Long and **E Casey**, Yale University, New Haven, CT, USA

doi:10.1006/rwfs.2000.0741

Introduction

This article focuses on criminal activity on the Internet in the highly intangible world of 'cyberspace'. An understanding of the Internet and cyberspace is crucial to the forensic scientist working on Internet crime, as many of the problems associated with the preservation and use of digital evidence arise from the peculiarities of cyberspace itself. The term 'Internet' as commonly used today is defined, and the relationship between 'cyberspace' and the physical world is examined. Since we are exploring new territory, 'Internet crime' itself is defined and explained. An attempt is made to identify and classify various types of Internet crimes and to assess their frequency and seriousness. The frequent interaction between Internet and real-world crime is discussed. Finally, the task of preserving digital evidence is examined.

The Internet and Cyberspace

The term 'Internet' once referred to a particular distributed group of networked computers. Increasingly, however, it has come in common parlance to be used to mean the global network of computers, the network of networks which provides its users with worldwide connectivity and communication.

The Internet, understood properly, is not a venue. It is a physical networking technology which facilitates human interaction of all sorts in a place that has come to be called 'cyberspace', a term coined by William Gibson, in his 1984 science fiction novel *Neuromancer*, to describe the virtual space in which computer-based activity occurred. Internet crime occurs *on* the Internet, but *in* cyberspace. The borderless nature of cyberspace and the difficulty of defining this new place's location, or establishing its relationship to other physical locations, is one of the seminal problems in regulating criminal activity on the Internet.

The Internet is like an enormous spider web comprising thousands of smaller webs, permitting a continuous line to be drawn between any two points on any of the smaller webs. The 'World Wide Web', the relatively recent, graphically oriented form of publication which seems destined to become the dominant vehicle for Internet interaction, is aptly named.

The development, or perhaps colonization, of cyberspace has been likened to the development of the American frontier in the latter half of the nineteenth century. It is a strong analogy. In the early days of the Internet, cyberspace was populated, although quite sparsely, by technological pioneers, feeling their way through unknown territory. They tended to be strongly individualistic and, in general, disliked and distrusted rules. They relied instead for behavioral control on a common understanding of what was appropriate and acceptable, made possible because most of these early inhabitants shared a common intellectual framework and sense of purpose. Soon, however, as the potential of cyberspace as a tool for communication and commerce began to be better understood and its population skyrocketed, the need for a more sophisticated form of control, a system of law, became apparent. It is worth noting that, although the early citizens of cyberspace are an increasingly tiny percentage of the population of cyberspace, their attitude was the seed of what has come to be called the 'hacker ethic', a belief that information should be free, which is at the root of a substantial amount of today's Internet crime.

What is Internet Crime?

There is no commonly accepted definition of 'Internet crime', although clearly not all crimes involving the use of a computer are Internet crime. The financial records of a money-laundering conspiracy might be kept, for example, on a computer. The digital evidence contained on that computer would, of course, be essential to the successful prosecution of the crime, but this would not be an Internet crime.

For the purposes of this article, Internet crime is any criminal activity that either occurs on, or makes use of, the Internet. It is important to note that Internet crime is thus not restricted to crimes committed in cyberspace and whose effects are felt only in cyberspace. Often, criminal activity on the Internet is specifically intended to produce effects in the physical world, with the Internet serving merely as a tool to facilitate the crime and avoid detection and capture. For instance, cyberstalkers use the Internet in addition to more traditional forms of stalking and harassment,

such as telephoning the victim and going to the victim's home.

Most Internet crime is the cyberspace analog of a real-world crime. Laws against fraud, for example, apply to the same conduct in cyberspace as in the real world, and proof requires establishment of the same legal elements defined by the relevant statute. Other Internet crimes are unique to cyberspace. 'Denial of service' attacks on a particular Internet site are one example. Another is breaking into a computer across the network by such means as cracking passwords, which required specialized 'unauthorized access' legislation that is now common in most jurisdictions.

A tremendously complicating factor in defining Internet crime, quantifying it and assessing its impact is the international nature of the Internet. There is no one set of applicable laws in cyberspace. When one speaks of Internet crime it matters greatly whose definition of 'crime' is used. Many Internet activities, such as gambling, that are perfectly legal in some jurisdictions are outlawed in others. Yet all jurisdictions are subsumed by cyberspace. Identifying 'all' Internet crimes by type is thus impossible, except as pertaining to a specific legal jurisdiction. Here, as we attempt to examine Internet crime from a global perspective, we must focus on the activities most commonly accepted as illegal, or at least unacceptable and problematic, by most of the Internet community.

The following activities are largely accepted as criminal misuse of the Internet:

- theft of proprietary information;
- unauthorized interception of electronic communications;
- unauthorized access to a computer system;
- theft of computer services;
- denial of service;
- distribution of a computer virus;
- financial fraud;
- espionage;
- extortion;
- trafficking in child pornography;
- solicitation of minors;
- stalking;
- harassment or threats.

Some of these crimes, such as trafficking in child pornography, solicitation of minors and stalking, are basically traditional crimes committed with the help of the Internet. For instance, the Internet enables child pornographers rapidly to transmit sexually explicit images around the world, giving commercial pornographers access to a larger market and giving cottage collectors access to a global village in which to trade. The Internet also gives sexual predators access to large numbers of children for extended periods of time, giving them ample opportunity to gain their victims' trust and arrange a meeting in the physical world. Sexual predators often take advantage of the anonymity that the Internet provides and sometimes pose as children to gain their victims' trust.

It should not be assumed that Internet crimes are more benign than their traditional equivalents. Victims of Internet crime experience the same distress as victims of crimes in the physical world. Also, some Internet crimes, such as stalking and solicitation of a minor, can lead to physical world confrontations. Although it is difficult to assess the full scope of these problems, it is clear that they have serious consequences in the physical world and are increasing in frequency as the Internet becomes more widely used.

Cyberstalking

The term 'cyberstalking' refers to stalking that involves the Internet – working in much the same way as stalking in the physical world. In fact, many offenders combine their online activities with more traditional forms of stalking and harassment, such as telephoning the victim and going to the victim's home. Cyberstalkers harass their victims using a wide variety of Internet services, including e-mail, newsgroups, chat rooms and instant messages. As well as harassing victims first encountered in the physical world, cyberstalkers target individuals they have never met. Other cyberstalkers take a less direct approach to harassment, putting personal information about their victims on the Internet, encouraging others to contact the victims or even harm them.

In general, stalkers want to exert power over their victims, primarily through fear. The crux of a stalker's power is information about and knowledge of the victim. A stalker's ability to frighten and control a victim increases with the amount of information that he or she can gather about the victim. Stalkers use information like telephone numbers, addresses and personal preferences to impinge upon their victims' lives.

Since they depend heavily on information, cyberspace is an ideal environment for stalkers, giving them access to a great deal of information about a large pool of potential targets. Additionally, a cyberstalker can determine when their victims enter cyberspace and can monitor them surreptitiously. This ability to lurk in cyberspace and protect their identity in other ways makes the Internet an even more attractive place for stalkers.

Internet computer crime

Many countries have adopted the view that certain Internet crimes are sufficiently different from tradi-

tional crime to warrant discrete legislation. This subset of Internet crime might be labeled 'Internet computer crime' because the targets of such crimes tend largely to be computers themselves and the information they contain. **Table 1** describes the most common Internet computer crimes.

Past studies have shown that a significant percentage of computer crimes were committed by individuals inside the organization whose systems were being attacked. However, the number of external attacks has grown, becoming as numerous as internal attacks. Specifically, organizations are finding that the attacks on their systems are perpetuated through their connections to the Internet. Also, there has been a dramatic increase in the number of computer security breaches overall and a corresponding increase in financial losses. As a result, Internet computer crime has become such a problem that it is considered to be a national security risk by many countries. Note, however, that Internet computer crime is still a relatively minor cause of both data and financial loss (**Table 2**).

Several attempts have been made to categorize the subset of criminals who use the Internet to commit computer crime. For instance, Icove divides computer criminals into three categories: computer crackers, computer criminals and vandals. Another study proposed the categories described in **Table 3**. However, criminals often fall into multiple categories and are perpetually finding new ways to make use of the Internet, defying the boundaries imposed by these categories. As a result, this type of categorization can add confusion to an already complex subject.

Computer cracking

Individuals who break into computer systems with malicious intent are referred to as 'computer crackers'. Crackers gain unauthorized access to computer systems in a number of ways, as described in **Table 4**. Although it takes a certain degree of skill to find new ways to implement these attacks, once a new method of attack is developed, it is often made available on the Internet to enable individuals with a minimal amount of skill to implement the attack.

Computer cracking is viewed by some as a victimless crime. However, whether a computer cracker steals proprietary information from an organization, misuses a computer system, or deletes the contents of an individual's computer, people are affected in a very real way. If, for example, a computer cracker changes prescription information in a pharmacy database, tampers with critical systems at an airport, disables an emergency telephone service or damages other critical systems, the ramifications can be fatal.

Investigating Internet Crime

To investigate Internet crime effectively it is necessary to be ever cognizant of its dichotomy. As mentioned earlier, Internet crime occurs *on* the Internet but *in* cyberspace – the components, separated by physical space, that comprise the Internet are joined to create a seamless virtual space. Therefore, when investigating Internet crime it is necessary to collect evidence stored on and transmitted using computers and, at the same time, use that discrete evidence to reconstruct the crime as it occurred in its native, seamless environment. Without an understanding of the physical components that comprise the Internet, forensic scientists will have great difficulty acquiring and analyzing evidence. Without a solid understanding of cyberspace, forensic scientists will have great difficulty assessing the significance of evidence, reconstructing Internet crimes and understanding the criminal act as a whole.

Although this is not the place for a full discussion of how the Internet functions, a summary description is warranted, starting with some basic terminology. Computers that are connected to the Internet, generally referred to as hosts, communicate using a set of protocols collectively called TCP/IP (Transport Control Protocol/Internet Protocol). Remember that the Internet is comprised of many individual networks. TCP/IP is essentially the common language that enables computers on these individual, often dissimilar, networks to communicate. Computers that are connected to two or more of these networks and direct traffic between them are called routers.

Hosts that provide a service to other computers on a network are commonly called servers, and hosts that access these servers are called clients. Any host, even a personal computer in someone's home, can become a server – all that an individual has to do is install a piece of software. Some servers allow anyone to access their resources without restrictions (e.g. Web servers) while others (e.g. e-mail servers) only allow access to authorized individuals, usually requiring a user identifier and password.

Every host on the Internet is assigned a unique number, called an Internet Protocol (IP) address, to distinguish it from other hosts. Before information is sent through the Internet, it is addressed using the IP address of the destination computer, much like an envelope is addressed before it is submitted to a postal system. Routers use these IP addresses to direct information through the Internet to its destination. If the sender requires confirmation that the destination computer has received a transmission, the TCP will perform this task, resending information when necessary. Be aware that TCP performs other functions,

Table 1 Internet computer crime incident categories

Name	*Description*
1. Compromise	Replacing or modifying part of a computer system to facilitate unauthorized access or perform malicious actions
2. Covert channels	This activity usually involves smuggling data (e.g. eavesdropped information such as captured 'sniffed' packets) out of an organization by hiding the outbound data stream (either having it (1) 'masquerade' as innocuous network traffic, (2) encrypting it, (3) encapsulating it as data inside another network protocol – also known as 'tunneling', (4) and/or using 'steganogrpahy' – a branch of cryptography where data is hidden inside other data, such as a secret message inside an image file or audio stream)
3. Eavesdropping	Sniffing network traffic and observing traffic to and from terminals as well as keyboards and monitor screens. Often a compromised machine is controlled remotely via the network, the network interface being put into a 'promiscuous mode' where it is used to covertly capture packet traffic
4. Denial of service	A purely malicious attack with the purpose of disabling access or availability of a resource (computing cycles, network bandwidth, disk space, data, etc.). Often abbreviated as DoS. Denial/disruption of service attacks may occur at the lower network layers (e.g. packets) or at the application layer (e.g. 'e-mail bombs') and may be quantitative (e.g. bombarding a network with packets to degrade bandwidth) or qualitative (a targeted attack on a Web server designed to crash or otherwise disable the specific service)
5. Harassment	Also referred to as 'cyberstalking'. Repeated unwanted communication from one individual to another. Harassment may be via private e-mail, public mailing lists, Usenet newsgroups, 'bulletin boards', instantaneous messaging mechanisms, interactive 'chat' as well as other forms of audio/video/text messaging/conferencing
6. Hijacking	The 'takeover' of, or 'piggyback' on to, a legitimate and previously established network session by a malicious individual or program. Data transfers may be redirected or modified, files damaged or stolen, login accounts compromised or malicious actions executed on the target system. In most cases the user loses total control of their 'session' (e.g. login, file transfer or Web browsing) and never regains it. Hijacking attacks are rare and sophisticated
7. Intrusion	Also known as a 'break-in', this involves obtaining unauthorized access to a computer system or network. The intruder may actually login as if on a terminal or they may just gain access to a specific network service (such as a file, e-mail or Web server)
8. Malicious software	Executables in native binary form (e.g. DOS/Windows .EXE and .COM files) as well as programs and program fragments written in scripting and macro languages. Also referred to as 'malware'. Some of the most common malicious programs (malware) are:
8a. Back door	A program which opens up access (login, dialup, network) to a machine from the outside to allow an unauthorized intruder into the machine
8b. Logic bomb	A program which is designed with a 'logic' trigger for activation of the malicious code or mode. The 'logic' is a particular condition or set of conditions. Similar to a 'time bomb'
8c. Time bomb	A program which is designed with a date/time based trigger for activation of the malicious code or mode. A 'time bomb' malicious program may be a virus, trojan or a legitimate program which stops working at a predetermined date/time. See also 'logic bomb'.
8d. Trojan	A program which does something (malicious) other than what is expected. Also known as 'Trojan horse'.
8e. Worm	A program which propagates itself (without external help), often from one computer to another across a data network (e.g. via a LAN – Local Area Network or WAN – Wide Area Network). A worm is usually standalone – not attached or in a symbiotic or parasitic relationship with another program
8f. Virus	A program which replicates itself. Parasitic, it usually attaches itself to, overwrites or replaces part of another program (the 'host' program) to spread. Major virus types are: • *Boot Sector* An infection of the boot sectors of floppy diskettes and other 'bootable' media (fixed or removable) as well as the partition sectors (e.g. MBR – master boot record) and/or DOS boot sectors of hard disks. The normal bootstrap code on the disk is replaced by a malicious version during an infection. This code runs before an OS (operating system) is loaded and run. These viruses used to be the most common, but have now been replaced in frequency by 'macro viruses' • *Companion* Virus relies on the fact that the MS-DOS command line interpreter (COMMAND.COM) invokes .COM files before .EXE files with the same base filename. • *Dropper* A program used to 'drop' a virus on to a system. Often a desirable game or free utility program available for Internet download, the dropper program or installer contains a dangerous payload – a malicious program (e.g. a virus or Trojan) is also installed on the system • *Macro* Virus written in an application's high level 'macro' or scripting language. The code is actually a part of a document or data file. The most common 'macro' viruses involve infected Microsoft Office application files (Word documents, Excel spreadsheets, etc.). 'Macro viruses' are typically spread by documents which are either e-mailed or downloaded from the Web or a network file repository

Table 1 continued

Name	*Description*
	• *Program virus* Viruses which attach themselves to either system or ordinary executable programs on disk. On DOS and Windows computers the files infected usually have filename extensions of .EXE, .COM, .OVL, .DRV, .SYS, .BIN. Other lesser affected file types have extensions of .DLL or .VXD. • *Multipartite* Viruses which can operate in either 'boot sector' or 'program' virus mode (e.g. infect either a boot sector or a program on disk)
9. Piracy	Unauthorized copying and distribution of software or other copyrighted material (e.g. audio, video, graphics, etc.). There are organized and unorganized groups on the Internet involved in software piracy (of commercial software and video game ROMs) as well as the illegal duplication of other intellectual property. The Internet jargon term for this illicit material is 'warez' (from 'wares')
10. Scanning/probing	Testing a networked computer for vulnerabilities (typically vulnerable services, but also checking for vulnerable accounts and passwords) remotely via the network. Criminality varies according to the law of each country
11. Spamming	Sending unsolicited messages, usually e-mail. Usually commercial in nature (e.g. advertising or solicitations), 'spam' messages are often sent in 'bulk' to multiple e-mail addresses. Harvesting, trading and buying/selling lists of e-mail addresses is now a business on the Internet. Legislation has been enacted in the United States to make many forms of 'spamming' illegal.
12. Spoofing	Forging/synthesizing data and/or masquerading identity at several levels: • *IP spoofing* (there is also UDP and TCP level spoofing) involves 'forging' data within packets which are then transmitted over TCP/IP networks (such as the Internet). The source of the message has usually been modified so that the real origin cannot be discovered and often is pretending to have been sent from a different real source • *DNS spoofing* involves the misdirection of Domain Name System records or servers. • *Web spoofing* is a passive attack at the application level in which a malicious Web server either (1) attempts to masquerade as another Web server or (2) 'traps' the Web browser user on the site and tricks him or her into believing they have left the site via a hyperlink – when they have not left the site and all data they are browsing as well as their responses are being passed to the malicious Web site. 'Frame' spoofing is another form of this. • *'Replay Attacks'* are a form of spoofing that involves reverse engineering fields of a captured sniffed network packet, modifying parts of the packet and retransmitting it
13. Theft of service	An attack with the purpose of obtaining unauthorized access to a resource (computing cycles, network bandwidth, disk space, data, etc.). In some cases the motive behind the 'theft' is to avoid paying (for information, Internet access, telephone service, etc.); in other cases the motive is to obtain access to a resource that is restricted or denied to the perpetrator

such as breaking information into packets, and that there are other protocols in the TCP/IP family, such as the User Datagram Protocol (UDP), the Internet Control Message Protocol (ICMP) and the Address Resolution Protocol (ARP). It is also worth noting that TCP/IP enables other protocols like Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP) to transmit e-mail and Web pages, respectively.

Table 2 Causes of financial and data loss

Percent	*Description*
55	Human error
20	Physical security problems (e.g. natural disasters, power problems)
10	Dishonest employees (employees who profit from their attacks)
9	Disgruntled employees
4	Viruses
1–3	Outsider attacks

Source: Computer Security Institute.

Whether a host is used by an individual at home to browse the Web or is used by a large corporation to manage its employees' e-mail, it contains information about the Internet activities of the people who use it. Even when information is deleted and overwritten it can be recovered. Knowing where and how to look for this information is a crucial skill when investigating Internet crime. When an Internet crime just involves e-mail, an understanding of TCP/IP is useful but not essential – investigators might only require a basic understanding of e-mail to perform an effective investigation. However, most Internet crime requires investigators to be familiar with the underlying computer and networking technology. For instance, to investigate computer intrusions effectively, a solid understanding of TCP/IP and the operating system(s)

Table 3 Computer crime perpetrator categories

Class	*Description*	*Primary motive(s)*
Corporate spies	Agents acting on behalf of corporations	Technical or business information
Hackers	Usually young (teenage or in twenties) males	Challenge, status, fame
Insiders	Employees or ex-employees	Revenge, personal gain or use
Professionals	Individual or 'organized' criminals	Information for financial gain
Spies	Agents of foreign governments	Strategic or political information
Terrorists	Amateur 'hackivists' or professional government-sponsored 'information warriors'	To cause damage or fear to achieve political objectives
Vandal	Individual or group who may or may not be angry (aggrieved party) at intended target	Damage, possibly for revenge

Source: Howard JD (1997) *An analysis of security incidents on the Internet 1989–1995*. PhD thesis, Carnegie Mellon University.

involved is required. A comprehension of the technology involved will enable investigators to recognize, collect, preserve and analyze evidence related to Internet crime.

Evidence on the Internet

When the Internet is involved in a crime, evidence is often distributed on many computers, making it infeasible to collect all of the hardware, or even the entire contents of a network, as evidence. Also, bear in mind that evidence is often present on the Internet for only a split second, making it difficult to collect. Additionally, encryption software is becoming more commonplace, allowing criminals to scramble incriminating evidence using very secure encoding schemes, making it unreadable. Furthermore, unlike crime in the physical world, a criminal can be in several places on a network at any given time. Given the many challenges that evidence on the Internet presents, a solid comprehension of how the Internet functions and how the principles of forensic science can be applied to computer networks is a prerequisite for anyone who is responsible for locating evidence and collecting it in a way that will be accepted in a court of law.

Evidence classification and individualization

In common with other forms of physical evidence, evidence on the Internet can be classified and individualized. Being able to classify and individualize evidence of an Internet crime, or the tools that were used to commit an Internet crime, can be helpful in an investigation. For example, when investigating a computer intrusion, class and individuating characteristics of the tools that were used can be helpful in determining which vulnerability was exploited, linking cases, finding additional evidence and assessing the skill level of the intruder. Some technical skill is required to closely analyze digital evidence, and knowledge of computer programming is sometimes required to decompile a program and find its class and individuating characteristics.

Virus research laboratories have classification systems for certain kinds of malicious software. However, a more comprehensive body of research classifying all forms of evidence that exist on the Internet has yet to be developed. Currently, the primary means of classifying and individualizing evidence on the Internet is through direct comparison with other samples obtained from past cases or loosely organized, incomplete archives.

Table 4 Computer crime primary internet intrusion attack methods

Attack vector name	*Description*
Authentication bypass	Gaining access while avoiding standard authentication
Authentication failure	Taking advantage of authentication systems which 'fail open'
Buffer overflows	Exploiting stack memory overwriting in networked server programs
Password cracking	Brute-force, reverse-engineering and 'dictionary'-based methods used to discover account passwords
Password sniffing	Capturing account passwords via a network 'tap'
Session hijacking	Piggybacking on authorized user connections from the Internet into internal hosts and networks
Social engineering	Impersonation of authorized personnel to gain access or network passwords
Spoofing	Having a computer masquerade as a different 'trusted' computer to gain access
Trojan horses	Malicious programs such as BackOrifice can provide 'back doors' (unauthorized avenues for access) into hosts from the Internet

See also: **Computer Crime**. **Electronic Communication and Information**.

Further Reading

Casey E (1999) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. London: Academic Press.

Cheswick WR and Bellovin SM (1994) *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, MA: Addison-Wesley.

Dunne RL (1994) Deterring unauthorized access to computers: controlling behavior in cyberspace through a contract law paradigm. *Jurimetrics: American Bar Association Journal of Law, Science, and Technology* **35**(1):1–15.

Garfinkel S and Spafford G (1996) *Practical UNIX and Internet Security*, 2nd edn. Sebastopol CA: O'Reilly.

Garfinkel S and Spafford G (1997) *Web Security and Commerce*. Sebastopol, CA: O'Reilly.

Hardy IT (1994) The proper legal regime for 'cyberspace'. *University of Pittsburgh Law Review* **55**(4): 993–1055.

Hollinger RC (1997) *Crime, Deviance and the Computer*. Brookfield, VT: Dartmouth.

Icove D, Seger K and VonStorch W (1995) *Computer Crime: A Crimefighter's Handbook*. Sebastopol, CA: O'Reilly.

Pipkin DL (1997) *Halting the Hacker: A Practical Guide to Computer Security*. New York: Prentice Hall.

Rosenblatt KS (1995) *High-Technology Crime: Investigating Cases Involving Computers*. San Jose, CA: KSK.

Russell D, Gangemi GT Sr (1991) *Computer Security Basics*. Sebastopol, CA: O'Reilly.

Stephenson P, (2000) *Investigating Computer-Related Crime: A Handbook for Corporate Investigators*. Boca Raton, FL: CRC Press.

Wilding E, (1997) *Computer Evidence: A Forensic Invertigations Handbook*. London: Sweet & Maxwell.

INVESTIGATIVE PSYCHOLOGY

D Canter, University of Liverpool, Liverpool, UK

doi:10.1006/rwfs.2000.0780

Introduction

The domain of investigative psychology covers all aspects of psychology that are relevant to the conduct of criminal or civil investigations. Its focus is on the ways in which criminal activities may be examined and understood in order for the detection of crime to be effective and legal proceedings to be appropriate. As such, investigative psychology is concerned with psychological input to the full range of issues that relate to the management, investigation and prosecution of crime.

As Canter made clear, when he first labeled and introduced the term 'investigative psychology', its constituents can be derived from consideration of the sequence of activities that constitute the investigative process, which runs from the point at which a crime is committed through to the bringing of a case to court. This makes it apparent that detectives and others involved in investigations are decision-makers. They have to identify the possibilities for action on the basis of the information they can obtain. For example, when a burglary is committed they may seek to match fingerprints found at the crime scene with those of known suspects. This is a relatively straightforward process of making inferences about the likely culprit from the information drawn from the fingerprint. The action of arresting and questioning the suspect follows from this inference.

However, in many cases the investigative process is not so straightforward. Detectives may not have such clear-cut information but, for example, suspect that the style of the burglary is typical of one of a number of people they have arrested in the past. Or, in an even more complex example, such as a murder, they may infer from the disorder at the crime scene that the offender was a burglar disturbed in the act. These inferences will either lead them on to seek other information or to select from a possible range of actions, including the arrest and charging of a likely suspect.

Investigative decision-making thus involves the identification and selection of options, such as possible suspects or possible lines of inquiry, that will lead to the eventual narrowing down of the search process.